YEARBOOK OF INTERNATIONAL & EUROPEAN CRIMINAL AND PROCEDURAL LAW
Vol.3, 2024 Article 1

Internet and sexual abuse of minors. Towards a new proposal for regulation and protection of vulnerable people

Paul Chapman

DOI:10.5281/zenodo.13995563

Internet and sexual abuse of minors. Towards a new proposal for regulation and protection of vulnerable people

DOI:10.5281/zenodo.13995563

Paul Chapman, Ph.D, Criminal legal advisor, UK.

Abstract: The present paper aims to investigate the protection of online child abuse. The story so far is small from a regulatory and jurisprudential point of view within the European Union. The new proposed regulation will try to close the gaps of the past and pave the way for greater protection of the fundamental rights and above all of crimes having to do with the internet. New proposals, new problems, non-feasible solutions and/or even innovations in the sector are topics that will be addressed and based not so much on the doctrine and legislation under examination but more on the relevant jurisprudence which allows us to arrive at new analytical conclusions.

Keywords: sexual abuse of minors on the internet; vulnerable people; European Union law; CSAM; CSA; child pornography; vulnerable people; protection of fundamental rights; minors'

rights; chat control; ePrivacy; data retention; ICT; cyberspace; grooming.

Introduction

Fake news, hate speech, false profiles, photoshop, false Twitter, Instagram and Facebook with false statements, pseudo journalists with false news on the internet and cyberbullying are some of the daily elements at a global level that have made national and international legislators take a stand for address continuous technological development, especially the sexual abuse of minors on the internet.

The 2022 annual report of the Internet Watch Foundation (IWF) immediately comes into our hands and thoughts, which informs us about:

"(...) the number of reports relating to the dissemination of images and videos containing child sexual abuse. This material (CSAM) has doubled compared to 2019 levels (Dorotic, Johnsen, 2023)[1] and, in the European Union (EU) alone, the number of online child sexual abuse reports has gone from 23,000 in 2010 to over 72,500 in 2019, with a drastic worsening caused by the Covid-19 pandemic (...)"[2].

1https://www.ceop.police.uk/Safety-Centre/what-is-online-child-sexual-abuse/; https://www.unicef-irc.org/research/sexual-abuse-and-exploitation-of-children-through-the-internet-and-other-information/; Internet Watch Foundation, The Annual Report 2022: https://annualreport2022.iwf.org.uk/wp-content/uploads/2023/04/IWF-Annual-Report-2022_FINAL.pdf, p. 37.

2See the National Center for Missing and Exploited Children (NCMEC): https://www.missingkids.org/theissues/csam; EUROPOL, Exploiting Isolation: Sexual Predators Increasingly Targeting Children During COVID pandemic. A Further Increase in Sharing of Child Abuse Material Online, Sexual Coercion and Extortion of Children is Expected, 19 June 2020: https://www.europol.europa.eu/media-press/newsroom/news/exploitingisolation-sexual-predators-increasingly-targeting-children-during-covid-pandemic

Sensational numbers which, together with the phenomena of searching for child pornography material online, show that the lowering of the age of victims is an increasing phenomenon, especially among children of all genders between 3 and 13 years old[3], just as new technologies that also play an important role in the sector of solicitation as well as the phenomenon of financial extortion[4].

The sexual abuse and exploitation of minors, as well as the dissemination of child pornography of photos and more, constitute crimes that are included in Directive 2011/93/EU (Martellozzo, 2012) on the fight against sexual abuse and child pornography[5]. A phenomenon that is not only European but global as a challenge that requires attention to ad hoc action on the part of the EU and its Member States.

European work against online child sexual abuse

According to Articles 3, par. 3 and 5 TEU, the promotion and protection of human rights are part of the main objectives of the EU even before the entry of the Treaty of Lisbon in force which is part of an important stage for the interests of minors and the

3INHOPE, Annual Report 2022: https://inhope.org/media/pages/articles/annual-reports/14832daa35-1687272590/inhope-annual-report-2022.pdf pp. 38-39.

4Federal Bureau of Investigation (FBI). (2023, February, 23). International Law Enforcement Agencies Issue Joint Warning About Global Financial Sextortion Crisis.

5Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and exploitation of minors and child pornography, and replacing Council Framework Decision 2004/68/JHA, in OJEU L 335/1 of 17 December 2011.

principles they have international nature for the protection of one's rights (Garde, 2014; Lind-haldorsson, O'Donnell, 2015; Kisunaite, Delicati, 2021). Of the same spirit is Art. 24 CFREU (Peers and others, 2021)[6] which actually included the rights of the UN Convention on the Rights of the Child in New York of 1989 and the related optional protocols (Sutherland, 2016; Vandenhole, Türkelli, Lelmbrechts, 2019; Kilkelly, Liefaard, 2020)[7].

The CFREU states:

"(…) the right of children to the protection and care necessary for their well-being and, in compliance with the principle of the best interest of the child, that in all acts that concern them, whether carried out by public authorities or by private institutions, are of the best interests of the minor and must be considered paramount. An obligation of method and result is therefore established, by virtue of which the best interests of the minor must always be taken into consideration in balancing the other rights and interests at stake (...)" (Peers and others, 2021).

In the EU Strategy for a more effective fight against child sexual abuse 2020, the European Commission described:

"(...) the fight against child sexual abuse (CSA) as one of its priorities", i.e. as a global response to its growing threat both offline and online. The 2020 Strategy outlined a legal protection framework based on eight initiatives and the involvement of all stakeholders in the prevention, protection and support

6In the G.U.U.E. C 364/1 of 18 December 2000.

7United Nations, Convention on the Rights of the Child, United Nations General Assembly resolution 44/25, New York, 20 November 1989. Optional Protocols to the Convention on the Rights of the Child on the Involvement of Children in Armed Conflict and on the Sale of Children, Child Prostitution and Child Pornography, United Nations General Assembly, Resolution A/RES/54/263, 16 March 2001. Optional Protocol to the Convention on the Rights of the Child on the Involvement of Children in Armed Conflict, United Nations General Assembly, Resolution A/RES/54/2643, 20 May 2000. Optional Protocol to the Convention on the Rights of the Child on a Communications Procedure, United Nations General Assembly, resolution A/RES/66/138, 27 January 2012.

of minors (Ramiro and others, 2019; Ali, Abou Haykal, Youssef, 2021)[8].

On 24 March 2021, the European Commission adopted the EU Strategy on the rights of the child:

"(...) a first global strategy on the rights of children which aims to place children and their best interests at the center of EU policies, with the general ambition of making their lives as good as possible in the European Union and around the world through strengthened protection measures against all forms of violence, including online abuse and exploitation[9] (...) the invitation made by Commission on information and communications technology (ITC) companies to implement their commitment to detect, report and remove illegal online content, with particular attention to child sexual abuse, from their platforms and services (…)".

Promote a European model for digital transformation, which puts people at the centre, is based on European values and EU fundamental rights. This reaffirms universal human rights and brings benefits to all people, businesses and society as a whole. The recent proposal for a European Declaration on Digital Rights and Principles has included among its objectives the commitment to promote a safe digital environment for children and protect them from harmful and illegal content, exploitation, manipulation and online abuse as well as prevent cyberspace from being used to commit or facilitate crimes[10].

The documents presented and the recognition of the role played

8Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, EU Strategy for a more effective fight against child sexual abuse, COM(2020) 607 final, Brussels, 24 July 2020, p. 2.

9Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, EU Strategy on the Rights of the Child, Brussels, 24 March 2021, COM(2021)142 final.

10Joint declarations, European Parliament, Council, European Commission, European Declaration on Digital Rights and Principles for the Digital Decade, 23 January 2023, in OJ. C 23/1, p. 22, letter. c) and d).

by hosting service providers as well as the communication state that:

"(...) responsible behavior is fundamental for the construction of a safe online environment in which the exercise of rights and fundamental freedoms are guaranteed" (Taddeo, Floridi, 2017; Wilman, 2020).

Faced with an increase in sexual abuse of minors in cyberspace, some providers have begun to voluntarily use specific technologies for detecting, reporting and removing CSAM. Already in 2012 Facebook had started an analysis of unusual messages on its platform to identify cases of solicitation of minors (Menn, 2012). Microsoft worked on the development of PhotoDNA, a technology that helps identify and remove known images of child exploitation, now used by organizations around the world and, in August 2021, Apple announced the launch of a new initiative for the detection of known child pornography material, which was then postponed due to the strong opposition received (Wakefield, 2021).

Within this framework, it was noted that the providers presented, the diversity of the measures implemented as well as the quality of the reports had insufficient results[11]. The limited nature of similar measures especially by some Member States of

11Commission Staff Working Document, Impact Assessment Report Accompanying the Document Proposal for a Regulation of the European Parliament and of the Council Laying Down Rules to Prevent and Combat Child Sexual Abuse, SWD(2022)209 final, Bruxelles, 11 May 2022.

the EU, such as: Germany[12], France[13], Holland[14] and Austria[15] allow us to speak for the adoption of national regulations that combat and address online child abuse. Are these sufficient measures? Certainly not, given that the phenomenon is still in the evolutionary stage. Measures that do not follow a single model and which risk the fragmentation of a single digital market for services, thus determining the need for legislative harmonization to remove cases of sexual abuse of minors online from the national and European context and at EU level by developing a regulating digital services and eliminating existing obstacles[16].

On 11 May 2022, the Commission presented the proposal for a CSAM regulation stating that:

"(...) uniform rules to combat the misuse of information society services concerned for the purposes of online child sexual abuse in the internal market in order to establish a clear and harmonized legal framework for preventing and combating online child sexual abuse (…)".

12See the Netzwerkdurchsetzungsgesetz or Network Enforcement Act (NetzDG) of 2018, the Gesetz zur Bekämpfung von Rechtsextremismus und Hasskriminalität im Internet of 30 March 2021.

13See la Loi n. 2020-766 du 24 juin 2020 visan à lutter contre le cotenus haineux sur internet. The Projet de Loi visant à sécuriser et réguler l'espace numerique du 5 juillet 2023 for other information see also: https://www.senat.fr/travaux-parlementaires/textes-legislatifs/la-loi-en-clair/projet-de-loi-visant-a-securiser-et-reguler-lespace-numerique.html

14See, Wet bestuursrechtelijke aanpak online kinderpornografisch materiaal of 16 February 2021: https://www.raadvanstate.nl/adviezen/@127611/w16-21-0337/

15See the Federal Act on measures to protect users on communication platforms (Communication Platforms Act) of 1st January 2021: https://www.ris.bka.gv.at/Dokumente/Erv/ERV_2020_1_151/ERV_2020_1_151.html

16Commission Staff Working Document, Business Journey on the Single Market: Practical Obstacles and Barriers, SWD(2020)54 final, Bruxelles, 10 March 2020, p. 29 ss.

The introduction of risk assessment and mitigation obligations complemented by obligations for the detection, reporting and removal of CSAM, which providers, who offer certain types of online services in the digital single market, must comply. Since its presentation the CSAM proposal has aroused quite a few criticisms and doubts about its actual ability to succeed in establishing a right balance between the needs of protection of minors and their rights, including online, and some fundamental rights and freedoms of other interested parties, in particular the privacy of users and providers of digital services[17].

The legal problems that arise with the presentation of this proposal are more or less precise and clear, requiring the current formulation of the legislation under discussion that is capable of establishing a balance between the rights and interests that are relevant in the context considered.

From Regulation (EU) 2021/1232 (so-called ePrivacy regulation) to the proposed CSAM regulation

The CSAM regulation aims to replace and clarify the temporary regime in the first steps that was introduced with the Regulation (EU) 2021/1232[18] (so-called ePrivacy regulation) where the

17Art. 1, par. 1, of the Proposal for a Regulation of the European Parliament and of the Council establishing rules for preventing and combating child sexual abuse, 11 May 2022, COM(2022)209 final.

18Regulation (EU) 2021/1232 of the European Parliament and of the Council on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal

exceptions to some provisions of the old Directive 2002/58/EC are addressed (so-called ePrivacy directive)[19] and are aimed at preventing and combating child pornography material that acts liberally on the internet and not only for the purpose of soliciting minors online. The derogation that was introduced with the ePrivacy Regulation sought to address and close the gaps in the ePrivacy Directive by guaranteeing privacy rights as well as the confidentiality of the processing of personal data in the sector dealing with electronic communications, thus determining the ad hoc provisions on the processing of personal data by providers of electronic communication services identifying, reporting and removing online child pornography material from their services (Koenig, Bartosch, Braun, Romes, 2009; Gonzàlez Fuster, 2014; Zech, 2021).

The ePrivacy regulation laid the foundations for the data concerning the detection of similar practices that had been entrusted mainly to the voluntary action of some suppliers, based on specific technologies (e.g. hashing technology for images and videos, classifiers, artificial intelligence for analysis of the text or data on traffic), which have proven to be

communications services for the processing of personal and other data for the purposes of combating online sexual abuse of minors, in the Official Journal. L 274/41 of 30 July 2021.

19Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 on the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), in Official Journal. L 201/37 of 31 July 2002.

fundamental for the identification of victims, the reduction of the further spread of child pornography material and the identification of the perpetrators of the crimes. These activities, however, risked interfering with some provisions of the ePrivacy Directive, which lacks an explicit legal basis for the voluntary processing of content or traffic data for the detection of CSA cases[20].

Reporting and removal of CSAM according to Art. 15 of Directive 2002/58/EC is based on legislation that is adopted by Member States to limit rights, obligations (articles 5 and 6) and protect the confidentiality of electronic communications and traffic data. Specific legislative measures of a national nature and the ePrivacy Directive have deprived communication service providers of the legal basis for carrying out direct actions on sexual abuse of minors and in their own services[21].

Regulation (EU) 2021/1232 through the derogation, operational from 2 August 2021 until 3 August 2024, to Articles 5, par. 1[22]

20Regulation (EU) 2021/1232 of the European Parliament and of the Council on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purposes of combating online sexual abuse of minors, op. cit.

21Regulation (EU) 2021/1232 of the European Parliament and of the Council on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purposes of combating online sexual abuse of minors, op. cit., 10th recital.

22"(…) Member States shall ensure, through national legal provisions, the confidentiality of communications carried out via the public communications network and publicly accessible electronic communications services, as well as the related traffic data. In particular, they prohibit the listening, collection, storage and other

and 6, par. 1[23] of the ePrivacy Directive which allowed providers of interpersonal and number-independent communication services (NI-ICS)[24]:

"(...) to continue to use specific technologies for the processing of personal and other data to the extent strictly necessary to identify, report and remove online child pornography material from their services (art. 1) (…)".

Indiscriminate monitoring of private communications has been introduced which has to do with the compatibility of the measure with the right to privacy and as has been addressed and foreseen by the Council of Europe[25] and the European Data Protection Supervisor (EDPS)[26]. The process followed was the one foreseen from 2017, where the regulation presented in a problematic way:

"(...) the inability to achieve the necessary balance pursuant to Articles 7 and 8 of the Charter between the right to respect for private life and data

forms of interception or surveillance of communications, and related traffic data, by persons other than users, without the latter's consent, except when authorized. Legally pursuant to Article 15, paragraph 1. This paragraph does not prevent the technical storage necessary for the transmission of the communication without prejudice to the principle of confidentiality (…)".

23"(…) traffic data relating to subscribers and users, processed and stored by the provider of a public network or a public electronic communications service must be deleted or made anonymous when they are no longer necessary for the purposes of transmitting a communication, without prejudice to paragraphs 2, 3 and 5 of this article and article 15, paragraph 1 (…)".

24Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (OJ L 321/36 of 17 December 2018.

25Council of Europe, Respecting Human Rights and the Rule of Law when Using Automated Technology to Detect Online Child Sexual Exploitation and Abuse, Indipendent Experts' Report, June 2021: https://rm.coe.int/respecting-human-rights-and-the-rule-of-law-when-using-automated-techn/1680a2f5ee.

26EDPS, Opinion 7/2020 on the Proposal for temporary Derogations from Directive 2002/58/EC for the Purpose of Combating Child Sexual Abuse Online, 10 November 2020: https://edps.europa.eu/sites/default/files/publication/20-11-10_opinion_combatting_child_abuse_en.pdf.

protection of users of services falling within the scope of the ePrivacy regulation and the need to protect children online, both for the risk of a high rate of assessment errors of the different technologies used. The text of Art. 3 of the 2021 Regulation provides for some conditions for the application of the aforementioned rules by suppliers. In particular, that the data processing is strictly necessary for the intended purposes, proportionate and an interpersonal communication service that does not connect to publicly assigned numbering resources - i.e. one or more numbers that appear in a national or international numbering plan - or which does not allow communication with one or more numbers appearing in a national or international numbering plan (art. 2, par. 7) (...) limited to the technologies used and data on content and traffic (par. 1, letter a, sub i). Suppliers are required to ensure that the technologies used, previously assessed by the national authorities (para. 1, letters c) and d)), comply with the state of the article of the sector, the least intrusive on privacy (letter b) and sufficiently reliable to limit the rate of errors (letter e). The preparation of adequate procedures and appeal mechanisms to ensure that the people affected by the aforementioned measures can present a complaint to suppliers and obtain rectification of any errors, if certain contents have been incorrectly qualified as CSAM (par. 1, letter. g), sub ii); which guarantee that the material has not been previously identified as online child pornography or that the solicitation of minors has not been reported to the authorities or organizations to combat child sexual abuse without prior human confirmation (sub iii); the provision of adequate procedures and redress mechanisms so that users can submit complaints (sub iv); that they are informed of the impact of the use of the derogation on the confidentiality of communications (sub v), as well as the methods for submitting appeals, the possibility of submitting a complaint to the supervisory authority and the right to a judicial appeal if their content has been removed (sub vi) (…)"[27].

It is a certain fulfillment of the conditions that guarantee the proportional nature of the limitation of rights that respect private life and protect personal data that determine the application of the derogation. The regulation also presents many perplexities. In the context of the European Parliament some groups contested the legislation which claimed that the protection of

27EDPS, Opinion 7/2020 on the Proposal for temporary Derogations from Directive 2002/58/EC for the Purpose of Combating Child Sexual Abuse Online, op. cit.

minors exposes other users of the services it involves to violations of their fundamental rights when in a general and indiscriminate way private communications are unacceptable and that they harm the right to private life[28]. Online child sexual abuse proves insufficient given the small number of providers who resort to it[29]. The proposed CSAM regulation was based on Article 114 TFEU (Blanke, Mangiamelli, 2021) and provided for measures that guarantee the functioning of the internal market. The CSAM proposal:

"(...) aims to eliminate existing barriers to the provision of the services concerned in the digital single market and to combat sexual abuse of minors perpetrated through improper use of information and communication services (...) a clear and harmonized legal framework on this matter through the introduction of obligations on information society service providers who offer such services in the EU regardless of their main place of establishment (Article 1, paragraph 2 of the proposal) (...) nor identified as such (so-called "new") and the solicitation of minors (so-called "grooming") (…)"[30].

Art. 3 requires:

"(...) to evaluate the possible risks of improper use of their services for the spread of CSAM or solicitation (par. 1), taking into account the cases already identified as such (par. 2, letter a), the existence of a strategy and functionality to counteract similar risks (letter b), the way in which the service is designed, managed and used by users (letter c) and d)), the age of minors who use the service (letter e), sub ii) and the presence of features that may give rise to the risk of grooming (sub iii) (…). Providers will be able to adopt effective, proportionate and targeted mitigation measures in relation to the identified risk and applied in a diligent and non-discriminatory manner (art. 4) (…). Will have to report on the outcome of the assessment and the

28Directive 2002/58/EC of the European Parliament and of the Council regarding the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purposes of combating sexual abuse on minors, A9-0258/2020, 11 December 2020, p. 42.

29COM(2022)209 final, p. 2-3.

30COM(2022)209 final, p. 4.

related mitigation measures to the coordinating authorities designated by the Member States, who will determine whether the risk assessment and the related mitigation measures mitigation comply with the provisions of Articles 3 and 4; (art. 5) (...) software application shop providers are required to evaluate whether the applications for which they act as intermediaries present the risk of being used for solicitation purposes and, if this is significant, they must implement reasonable measures, identify minor users and prevent them from accessing the service in question; (art. 6) (...) to ask the competent judicial authority of the Member State that designated it to issue an "order of detection" towards a provider of hosting services or interpersonal communication services falling within the jurisdiction of the state in question; (art. 10) to detect cases of CSA on a specific service if the coordinating authority deems that there is a significant risk of its improper use[31] (…) the mere observation of such a risk is not considered a sufficient reason to issue a detection order, considering the disproportionate consequences that it could produce on the rights and legitimate interests of other interested parties (...) the competent authority evaluates objectively, diligently and on a case-by-case basis the probability and severity of the potential negative consequences of improper use of the service and the effects on fundamentals rights of the other actors involved before proceeding with issuing the order, as well as the technological and financial capabilities of the provider, in order to avoid the imposition of excessive charges (...)"[32].

Continuing by specifying that:

"(...) the detection order must be identified and specified by the competent authority in such a way as to limit the negative consequences for the rights and legitimate interests of all interested parties, so as to guarantee a fair balance between the fundamental rights at stake (par. 8) (…) the risk is limited to an identifiable part or component, the coordinating authority and the independent judicial or administrative authority must ensure that the measures requested are applied only with respect to this part or component (letter a), proportionate and effective guarantees are in place (letter b), and the period of application of the order is limited to what is strictly necessary (letter c); (…) to the EU Agency for Prevention and the fight against child sexual abuse ("EU Center on Child Sexual Abuse" or "EU Centre") and inform the user concerned, indicating the reason for the report and its

31In relation to child pornography material: "(...) a similar risk exists where there is evidence that the service has been used in the last 12 months, to a significant extent, for the dissemination of known CSAM (para. 5) (...) concerns the new material, a significant risk exists if there is evidence that the service has been used, to a significant extent, in the last 12 months for the dissemination of new CSAM (…)" (para. 6).

32COM(2022)209 final, 22th recital.

consequences as well as the possible appeal tools available to you (art. 12, par. 1 and 2); (...) following diligent assessment, the coordinating authority of the place of establishment identifies a case of CSAM may request the competent judicial authority of the Member State that designated it to issue a "removal order" and a "blocking order" against a hosting and Internet access service provider. As a result of any removal order, the provider concerned will have to disable or remove access in all Member States to one or more specific elements of the material in question within 24 hours (art. 14, par. 1 and 2), unless it is impossible due to causes of force majeure - including technical or operational reasons (par. 5) - or due to manifest errors or insufficient information for execution (par. 6); (...) in accordance with art. 16, the coordinating authority has the right to also request the issuance of a blocking order requiring the Internet access service provider to take reasonable measures to prevent users from accessing known child pornography material (par. 1), after evaluating a series of elements aimed at determining the existence of the conditions referred to in par. 4 (par. 2) (...) highlights that, before proceeding with the request for a blocking order, the coordinating authority must verify that the service in question has been used in the last 12 months and to a significant extent to access or attempt to access child pornography material indicated by the uniform resource identifiers referred to in art. 44 (par. 4, letter a); that the order in question is necessary to prevent the spread of child pornography material, protect the rights of victims and encourage the implementation of a provider policy aimed at avoiding the risk of such spread (letter b); that the uniform identifiers indicate the existence of child pornography material to a sufficiently reliable extent (letter c); and that the reasons for issuing the order (...) considering the need to guarantee a fair balance between the fundamental rights of these parties, starting from the exercise of freedom of expression and information of users and freedom of enterprise of the provider (letter d). Furthermore, due to this need, it is established that the issuing of the blocking order is accompanied by the indication of effective and proportionate limitations and guarantees aimed at limiting the negative consequences and the duration of the period of application of the blocking to what is strictly necessary (par. 5, letters a) and b) (…)"[33].

The aim to be pursued is to ensure the EU center on child sexual abuse that responds to the definition of the responsibility of providers and contribute to the removal of obstacles to the national market[34]. The Union as a body that has legal personality

33COM(2022)209 final, 23th recital.
34COM(2022)209 final, p. 3.

(art. 41) attributes it to facilitating the implementation of the provisions of the regulation, collecting and sharing information that supports cooperation between interested parties, private and public in the field of prevention against the child abuse and in particular online (art. 40)[35].

Within this context, collaboration with Europol and other partner organizations of a relevant nature is necessary[36]. The EU Center ensures:

"(...) the establishment of databases of three types of indicators of online child sexual abuse: those to detect the dissemination of known child pornography material, those for new child pornography material and (...) for the solicitation of minors (art. 44, paragraph 1), as well as a database containing the reports transmitted by the providers of hosting and interpersonal communication (art. 45) (...) the aforementioned indicators must be applied by providers to comply with their reporting obligations and form the basis of any blocking orders so that consistency, efficiency and effectiveness are guaranteed and can be reduced to a minimum the risk of circumvention (...)"[37].

Privacy and personal data of users, protection of minors online within the proposed CSAM regulation

Of course, the proposed CSAM regulation is still an important innovation in the process of building a system of moderation and removal of illegal content online in the EU[38] as organized

35COM(2022)209 final, p. 40.

36U.S. National Centre for Missing and Exploited Children-NCMEC) and the International Association of Internet Hotlines-INHOPE).

37COM(2022)209 final, 33th recital, p. 44-45.

38"Illegal content" means "(…) any information which, in itself or in relation to an activity, including the sale of products or the provision of services, does not comply with the law of the Union or of any State Member compliant with Union law, regardless of the nature or specific object of that right": art. 3, letter. h) of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022

by the so-called Digital Services Act (DSA) (Woods, 2020) and which respects the approved proposal which constitutes a lex specialis[39]. The DSA responds to the need to define a system of rules that are harmonized for the moderation, removal and disabling of online content (De Streel, 2020; Bellanova, De Goede, 2022; Nunziato, 2023), as a delicate response proposal to the balancing between security needs and the protection of fundamental rights (Sartor, Loreggia, 2022).

The CSAM proposal implies a new regime enjoying some fundamental rights by those involved, such as users and providers of interpersonal communication services. The provisions contain the recognition of the challenges and problems that are connected to the obligations of the providers of these services, which prefigure the identification of a balance between different rights and freedoms, that are fundamental for the protection of this type of rights and the related subjects (Dunn, De Gregorio, 2023).

In ePrivacy Regulation, the proposed legislation appears very controversial given the dubious ability to guarantee the balance of the needs of the protection of minors and the protection of the

on a single market for digital services and amending Directive 2000/31/EC (Regulation on digital services), in OJEU. L 277/1 of 27 October 2022. This concept refers, in particular, to all information which under applicable law is in itself illegal, including incitement to hatred or illegal terrorist content and illegal discriminatory content, or which the applicable rules make illegal as they relate to illegal activities, such as the sharing of child pornography material (12th recital of the DSA).

39COM(2022)209 final, 8th recital.

rights and freedoms of the interested parties[40]. Some doubts are presented regarding the European Data Protection Board (EDPB)[41] and the European Data Protection Supervisor (EDPS) as a data protection supervisory authority in a joint opinion[42].

The doubts comply with the disclosure of art. 7 which is proposed by the CSAM as well as with Articles 7, 8 and 11 CFREU (Peers and others, 2021), which ensure and respect the protection of private life, personal data and freedom of expression. Such an order pursues general interests, where the prevention of the fight against sexual abuse of minors constitutes a serious crime that introduces limitations to the rights that are under consideration.

The proposal does not compromise considered rights that guarantee proportionality, that respects the objective pursued. According to Art. 52 CFREU:

"(...) any limitation on the exercise of the rights and freedoms recognized by (...) law and respect the essence of such rights and freedoms; essence that is

40European Digital Rights (EDRi) to the European Commission even before the presentation of the proposal of 11 May 2022, Scanning Private Communication in the EU, 9 February 2022: https://edri.org/wp-content/uploads/2022/02/EDRi-principles-on-CSAM-measures.pdf. European Commission (2022, June, 22). Uphold Privacy, Security and Free Expression by Withdrawing New Law: https://edri.org/wp-content/uploads/2022/06/European-Commission-must-uphold-privacy-security-and-free-expression-by-withdrawing-new-law.pdf.

41The European Data Protection Board (EDPB) is a European body that is independent in nature and brings together the national data protection authorities and the countries of the European Economic Area as well as the European Data Protection Supervisor (EDPS).

42EDPS-EDPB, Joint Opinion 4/2022 on the Proposal for a Regulation of the European Parliament and of the Council Laying Down Rules to Prevent and Combat Child Sexual Abuse, 28 July 2022: https://edps.europa.eu/system/files/2022-07/22-07-28_edpb-edps-joint-opinion-csam_en.pdf.

damaged when the right considered is emptied of its fundamental content, to the point of preventing its exercise (...)" (Svantesson, 2016; Voigt, Von Dem Bussche, 2017; Lenaerts, 2019; Dhont, 2019; Chander, 2020; Christakis, 2020; Flett, Wilson, Clover, 2020; Simon, 2020; Tracol, 2020; Voss, 2020; Liss, Peloquin, Barnes, Bierer, 2021; Peers and others, 2021)[43].

The limitations are possible and respond to the objectives of general interest that the Union pursues and which do not constitute objectives set in a disproportionate and unacceptable manner, damaging the substantial content of the right that is guaranteed[44].

Within this context, we recall the jurisprudence from the Court of Justice of the European Union (CJEU) as well as from the European Court of Human Rights (ECtHR). These are requirements which imply the interference with a specific right

43CJEU, CJEU, joined cases C-362/14 and C-362/14, Maximilian Schrems v. Data Protection Commissioner-Digital Rights Ireland Ltd of 6 October 2015, ECLI:EU:C:2015:650, published in the electronic Reports of the cases. See also in argument the next cases: C-288/12, Commission v. Hungary of 8 April 2014, ECLI:EU:C:2014:237, published in the electronic Reports of the cases. C-614/10, Commission V. Austria of 16 October 2012, ECLI:EU:C:2012:631, published in the electronic Reports of the cases. joined cases C-92/09 and C-93/09, Volker Volker und Markus und Markus Schecke GbR, Hartmut Eifert v. Land Hessen of 9 November 2010, ECLI:EU:C:2010:662, I-11063. C-28/08, Commission v. The Bavarian Lager Co. Ltd of 29 June 2010, ECLI:EU:C:2010:378, I-06055. joined cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and others of 8 April 2014, ECLI:EU:C:2014:238, published in the eletronic Reports of the cases, parr. 33 and 36; opinion 1/15 of 26 July 2017, ECLI:EU:C:2017:592, published in the electronic Reports of the cases, parr. 124 and 126. C-311/18, Facebook Ireland and Schrems (Schrems II) of 16 July 2020, ECLI:EU:C:2020:559, not yet published. joined cases: C-203/15 and C-698/15, Tele2 Sverige AB v. Post-och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and others of 21 December 2016, ECLI:EU:C:2016:970, published in the electronic Reports of the cases, par. 123. EDPS, Guidelines on Assessing the Proportionality of Measures that Limit the Fundamental Rights to Privacy and to the Protection of Personal Data, 19 December 2019.

44CJEU, C-393/19, Okrazhna prokuratura-Haskovo e Apelativna prokuratura-Plovdiv of 14 January 2021, ECLI:EU:C:2021:8, not yet published, par. 53.

which must be defined precisely and which leads to limitation of the exercise of the relevant right that is considered[45].

The relative terminology that was used appears to be the breadth of the evaluation, as we see for example, in art. 3 of the proposal which defines:

"(...) providers of hosting services and interpersonal communication services to identify, analyze and evaluate the risk of using the service for the purposes of sexual abuse of minors online and to try to minimize the risk identified by requiring the use of "reasonable and adequate mitigation measures" (articles 3 and 4 of the proposal) (…), par. 2 of the same art. 3 indicates which elements must be taken into consideration in the risk assessment. Some of the criteria lack clarity, leading to the risk that providers may interpret their obligations in different ways to the point of compromising the initial assessment on which any possible outcome depends on issuing a discovery order (…)"[46] (Davis, 2021).

The nature and characteristics of the technologies that use the implementation of a revelation order are not identified in detail. There is a gap regarding the meaning of: "sufficiently reliable detection technologies". It is an "error rate" relating to the detection to be considered acceptable in terms of balance between effectiveness and measures that are as least intrusive as

45CJEU, C-311/18, Facebook Ireland and Schrems (Schrems II) of 16 July 2020, op. cit., states that "(…) the requirement that any limitation on the exercise of fundamental rights must be provided for by law implies that the legal basis allowing the interference with such rights must itself define the extent of the limitation on the exercise of the right considered (…)". C-311/18, Facebook Ireland and Schrems (Schrems II) of 16 July 2020, ECLI:EU:C:2020:559, not yet published, par. 175. ECtHR Big Brother Watch and others v. The United Kingdom of 25 May 2021, par. 333 which is affirmed that: "(…) therefore essential to have clear, detailed rules on secret surveillance measures, especially as the technology available for use is continually becoming more sophisticated. The domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures (…)".

46COM(2022)209, p. 3.

possible (Kornelius, 2023)[47].

The proposed regulation recognizes a certain discretion of an interpretative nature to communication service providers, thus entrusting the relative choice of technologies to be used, the consequences and their functioning on the rights at stake.

In particular, the CJEU stated that:

"(...) this requirement does not exclude a formulation of this limitation in sufficiently broad terms to be able to adapt to different cases and possible changes in situations[48] and the possibility that it itself can, if necessary, specify its scope both with respect to the terms of the legislation in question and with respect to the systematic structure and objectives pursued by it, as interpreted in the light of the Charter of Fundamental Rights".

A circumstance that would therefore justify the recognition of communication services providers of a certain discretion in determining the concrete measures to be adopted in order to achieve the pursued objective[49].

Flexibility and discretion are exercised within a regulatory framework, which is detailed and provides for the relevant limits and guarantees, that are provided for the detection of orders and are issued by the judicial, administrative authorities independent of a Member State:

47EDPS-EDPB, Joint Opinion 4/2022 on the Proposal for a Regulation of the European Parliament and of the Council Laying Down Rules to Prevent and Combat Child Sexual Abuse, op. cit., pp. 16-17. See also the document: SWD(2022)209 final, op. cit., pp. 281- 283.

48CJEU, C-401/19, Poland v. European Parliament of 26 April 2022, ECLI:EU:C:2022:297, not yet published, par. 74.

49CJEU, C-401/19, Poland v. European Parliament of 26 April 2022, op. cit., C-817/19, Ligue des droits humains ASBL v. Conseil des ministres of 21 June 2022, ECLI:EU:C:2022:65, not yet published, par. 114.

"(...) after objective, diligent and specific assessment are prepared and executed under the supervision and with the support of other independent public authorities, in particular the EU Center and national data protection authorities (...)"[50].

The need for integration of elements that has to do with the limits of the rights involved respecting the technology and the providers, who made recourse and avoid the discretion, that recognizes and takes the form of an unlimited freedom of action and that gives rise to a control that favors interpersonal communications in an indiscriminate way.

Data retention through the relevant jurisprudence

When we talk about data protection we immediately remember Directive 2002/58/EC, which established:

"(...) the prohibition on the storage of data and metadata (traffic and location data) produced by telecommunications services (art. 5), placing the obligation on service providers to delete or make anonymous the traffic data relating to their users when such information became no longer necessary for the transmission of the communication itself or for billing (art. 6) (…)".

Within this context the ePrivacy directive stated that:

"(...) pursuant to art. 15, par. 1 giving Member States the power to adopt regulations aimed at limiting the rights and obligations of art. 6 if this restriction constitutes (...) a necessary, appropriate and proportionate measure within a democratic society for the protection of national security (i.e. state security), defence, public safety; and the prevention, research, detection and prosecution of crimes, or unauthorized use of the electronic communications system (...) has recognized Member States with broad autonomy with regard to determining conservation obligations, in the absence of specific conditions and limitations, thus opening up to a form of generalized data surveillance for security purposes (...) the excessive discretion attributed to national legislators together with the vagueness of the provision in art. 15 has given rise to a highly fragmented regulatory framework which has raised many

50Art. 7, parr. 1, 2 e 3 e art. 9, parr. 3 and 4 of CSAM.

problems (...)"[51].

Directive 2006/24/EC[52] intervened in this type of fragmentation as an act that contains rules that are harmonized with the conservation of data contained in electronic communications and which identified a transition from data protection to data retention (Feiler, 2010; Jones, Hayes, 2013).

Within this context, the regulation under investigation stated that:

"(...) measures to ensure that the data, if generated or processed in the framework of the provision of the communication services concerned (...) are retained in accordance with the provisions of this directive (art. 3, par. 1), to ensure their availability for the purposes of investigation, detection and prosecution of serious crimes (art. 1, par. 1) (…). A delimitation of the subjects whose metadata had to undergo conservation was not prepared, so that storage concerns all users and all electronic communications, without the need for a link between data retention and investigations or an authorization from a competent national authority. Furthermore, the conservation - the duration of which is established by the national legislator and must in any case be between six months and two years - must concern only the metadata indicated by art. 5, while data relating to the content of the communications are excluded (...)". (Bignami, 2006; Taylor, 2006; Guild, Carrera, 2014).

In particular, the CJEU did not examine the issue relating to the fight against the spread of child pornography material but elaborated on the preservation and monitoring of metadata which provide useful criteria for the evaluation of elements of

51Regulation (EU) 2021/1232 of the European Parliament and of the Council on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purposes of combating online sexual abuse of minors, op. cit.

52Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or public communications networks and amending Directive 2002/58/EC, in the Official Gazette. L105/54 of 13 April 2006.

the CSAM proposal.

In ruling of the CJEU: Digital Rights Ireland[53], the conservation of metadata poses the risk of serious damage to private life, being able to reveal information regarding the private life of the interested parties such as to generate of the latter the feeling that their private life is the object of constant surveillance (par. 37) in order to be legitimate, the conservation obligation must satisfy the requirements indicated by Art. 52 of the Charter, i.e. respecting the essential content of the rights at stake and being compliant with the principle of proportionality.

The retention of data constitutes a particularly serious interference with the right to respect for private life and the other rights enshrined in Art. 7 of the Charter, is not such as to undermine its essential content, since it does not allow us to become aware of the content of electronic communications (para. 39).

At the same time, such conservation is not even capable of compromising the essential content of the right to the protection of personal data referred to in art. 8 of the Charter since suppliers are required to respect certain principles of data protection and security (par. 40).

The profile of proportionality - for which the acts of the Union

53CJEU, joined cases C-362/14 and C-362/14, Maximilian Schrems v. Data Protection Commissioner-Digital Rights Ireland Ltd of 6 October 2015, op. cit., par. 39.

institutions must be suitable for achieving legitimate objectives pursued by the legislation in question and not to exceed the limits of what is suitable and necessary to achieve the objectives themselves-[54] requires to establish that the metadata constituted an additional tool for the competent authorities for ascertaining serious crimes and therefore their conservation was proportionate as it responds to the security objective pursued by the relevant legislation (para. 49)[55].

The directive judged as non-compliant the requirement of necessity and the lack of precise rules on the scope and application of the minimum requirements that are necessary for the data subjects and which guarantee the protection of their personal data against possible risk of abuse, as well as against any illicit access or use of such data (par. 54).

These are guarantees that become more important when personal data are subject to automatic processing (para. 55).

Directive 2006/24/EC obliges suppliers to generalized

54CJEU, C-343/09, Afton Chemical Limited v. Secretary of State for Transport of 8 July 2010, EU:C:2010:419, I-07027, par. 45. joined cases C-92/09 and C-93/09, Volker Volker und Markus und Markus Schecke GbR, Hartmut Eifert v. Land Hessen of 9 November 2010, ECLI:EU:C:2010:662, I-11063, par. 74. joined cases C-581/10 and C-629/10, Nelson and others v. Deutsche Lufthansa AG of 23 October 2012, ECLI:EU:C:2012:657, published in the electronic Reports of the cases, par. 71. C-283/11, Sky Österreich GmbH v. Österreichischer Rundfunk of 22 January 2013, ECLI:EU:C:2013:28, par. 50. C-101/12, Herbert Schaible v. Land Baden-Württemberg of 17 October 2013, ECLI:EU:C:2013:661, published in the electronic Reports of the cases, par. 29.

55CJEU, joined cases C-362/14 and C-362/14, Maximilian Schrems v. Data Protection Commissioner-Digital Rights Ireland Ltd of 6 October 2015, op. cit., parr. 39, 40.

conservation concerning any person and any means of electronic communication, as well as all traffic data without distinction, limitation or exception depending on the objective of fighting serious crime (para. 57).

In this regard, retention is not conditional on the existence of a relationship between the data and a threat to public security, nor any indications such as to suggest that the behavior of the persons concerned may have a connection, even if indirect or distant, with serious crimes (paragraphs 57 and 58).

Especially, the retention of data must be limited to a specific period of time and/or to a specific geographical area and/or to a group of specific people involved, in some way, in a serious crime or the retention of whose data could contribute to the prevention, detection or prosecution of serious crimes (par. 59).

The access of the competent national authorities to the data and their further use for the purposes of prevention, detection and investigation concerning crimes which could be considered sufficiently serious to justify interference with the fundamental rights referred to in Articles 7 and 8 of the Charter (par. 60).

It is considered that the regulation did not define a duration of storage based on objective criteria (par. 64 and 65) nor sufficient guarantees against possible illicit access and use of the data (par. 67 and 68)[56] (Granger, Irion, 2014).

56Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the

It is understood that the relevant legislation has not included as compliant the principle of proportionality according to Articles 7, 8 and 52, par. 1 CFREU (Peers and others, 2021). The Digital Rights Ireland decision and the CJEU via the Tele2Sverige ruling affirmed that:

"(...) a Member State may adopt legislation permitting the retention of metadata, provided that such retention is, with respect to the categories of data to be retained, the means of communication concerned, the persons concerned, as well as the expected retention period, limited to what is strictly necessary (par. 108) (...)"[57].

The relevant legislation has provided precise rules that define the measure considered, thus providing the people concerned with sufficient guarantees for any risks of abuse, which must meet the objective criteria by delimiting the scope of the measure and the subjects who are involved and who reveal the indirect connection with acts of crime and the related measures they must take in consideration.

Additionally, only the fight against serious crime is suitable to justify the conservation of metadata, without prejudice to the fact that this objective of general interest, however fundamental, cannot be considered sufficient to justify the need for a generalized and indiscriminate data conservation measure (paragraphs 102 and 103).

---

provision of publicly available electronic communications services or public communications networks and amending Directive 2002/58/EC, op. cit., parr. 54, 55, 57, 58, 59, 60, 67, 68.

57CJEU, joined cases: C-203/15 and C-698/15, Tele2 Sverige AB v. Post-och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and others of 21 December 2016, op. cit., par. 62.

Legislation that lacks the elements just indicated goes beyond the limits of what is strictly necessary and cannot be considered on the provision referred to in Art. 15, par. 1 of Directive 2002/58/EC read in light of Articles. 7, 8, 11 and 52, par. 1 of the Charter of Fundamental Rights (para. 107)[58].

The notion of "essence" in fundamental rights and how they are provided for in the CSAM

The contents of the interpersonal communication service are of interest, determine a form of monitoring that deals with data and has a general basis (Van Daalen, 2022). The essence of the rights that are considered must respect what has been foreseen and its restrictions (Brkan, 2018; Lenaerts, 2019). Proportionality respects the objective of identifying a balance between the rights and interests at stake. The doubts that respect the effects deriving from the issuing of the survey on the enjoyment of the right to private life and which as was foreseen by Article 7 CFREU (Peers and others, 2021) can be shared. We continue with the protection of personal data of Article 8 CFREU.

Some doubts exist only from the Legal Service of the Council of

58Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or public communications networks and amending Directive 2002/58/EC, op. cit., par. 108.

the EU in relation to the opinion expressed on 26 April 2023[59]. In particular, it was reported that:

"(...) the data in question constitute "personal data". This would allow the identification of the person or persons interested (…)".

The definition referred to in Art. 4, par. 1, of the General Data Protection Regulation (GDPR) (Liakopoulos, 2019)[60], "personal data" means

"(…) any information relating to an identified or identifiable natural person and the natural person who can be identified is considered identifiable, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more elements characteristic of his physical, physiological, genetic, mental, economic, cultural or social (…)",

since the screening of communications that would be implemented as a result of the aforementioned order presupposes the systematic access and processing of the information contained therein. This may allow, in a subsequent phase, the identification of all users affected by such automated analysis[61] (Liakopoulos, 2019).

Within this context, the CJEU through the "La Quadrature du Net" ruling of 6 October 2020 stated that:

59Opinion of the Legal Service, Proposal for a Regulation laying down rules to prevent and combat child sexual abuse-detection orders in interpersonal communications. Articles 7 and 8 of the Charter of Fundamental Rights-Right to privacy and protection of personal data-proportionality, 8787/23, Bruxelles, 26 April 2023.

60Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (Regulation general on data protection), in the OJ, L 119/1 of 4 May 2016.

61Opinion of the Legal Service, Proposal for a Regulation laying down rules to prevent and combat child sexual abuse-detection orders in interpersonal communications. Articles 7 and 8 of the Charter of Fundamental Rights-Right to privacy and protection of personal data-proportionality, 8787/23, op. cit.

"(...) to safeguard national security, required providers of electronic communications services to implement, on their networks, measures that allowed the automated analysis of traffic and location data" (Sajfert, 2020; Tracol, 2021; Cameron, 2021; Royer, Careel, 2021)[62].

Automated data analysis implies, for communication service providers electronic data subjects, the implementation of generalized and undifferentiated processing of data as defined by Art. 4, par. 2 GDPR[63] (par. 172).

A national regulation that authorizes such an analysis of metadata, as well as constituting an exception to the provisions of Art. 5 of Directive 2002/58/EC to guarantee the confidentiality of electronic communications and related data, constitutes an interference with the fundamental rights referred to in Articles 7 and 8 of the Charter and may have dissuasive effects on the exercise of freedom of expression established in the following art. 11 (par. 173).

The interference thus determined has a high level of gravity as it involves in a generalized and indifferentiated manner the data of all those who use the service in question, so that the automated analysis also operates towards users for whom there is no element that could lead one to believe that their behavior could

62CJEU, joined cases: C-511/18, C-512/18 and C-520/20, La Quadrature du Net and others v. Premier ministre and others of 6 October 2020, ECLI:EU:C:2020:791, not yet published, par. 171.

63"Processing" means: "(…) any operation or set of operations, carried out with or without the aid of automated processes and applied to personal data or sets of personal data, such as collection, recording, organisation, structuring, storage, adaptation or modification, extraction, consultation, use, communication by transmission, dissemination or any other form of making available, comparison or interconnection, limitation, cancellation or destruction (…)".

represent a connection, albeit indirect or remote, with a criminal act (par. 174)[64].

The ruling considers points in common with the order and objectives of the CSAM proposal, where according to the CJEU they are useful for the evaluation of interference and fundamental rights to give rise to the regime that prefigures the proposal under consideration. The order that reveals is addressed to a specific provider, where communication services of an interpersonal nature constitute a topic and this order considers and has a generalized and indiscriminate character.

In particular, a specific provider detects and determines a scan of all interpersonal communications that are related to this service or to the part or component that affects this service through automated tools[65]. Data processing is not limited and does not only include communications from users who respect the reasons that they are involved in a form of online child sexual abuse and which have an indirect link in cases of CSA. Any type of safeguard that has to do with such a risk is not based on discouraging the use of other services, purposes of sexual abuse of minors which constitute an extension of providers, who give rise to a surveillance that is permanent for

64CJEU, joined cases: C-511/18, C-512/18 and C-520/20, La Quadrature du Net and others v. Premier ministre and others of 6 October 2020, op. cit., parr. 172, 173, 174.

65Art. 8, par. 1, lett. d) of CSAM.

all services of interpersonal communication[66].

This is a serious interference with the rights at stake and in screening which does not concern metadata as noted in the “La Quadrature du Net” case and as a sensitive content with regards to invasive communication.

The related control of communications and the detection of child pornography requires the weakening and circumvention of information security measures using providers of interpersonal communication services: Signal, Telegram, Facebook Messenger, WhatsApp and Instagram Direct Message) and/or in particular the encryption that is called: “from point to point” (End-to-End Encryption or E2EE).

Message apps apply as a tool communications that leave the endpoints, i.e. the user's device, i.e. phone or computer, access to their content and the description key which is a device only for the sender and the recipient of the message (Lutkevich, Bacon, 2021).

The providers do not use an ad hoc technology but a technology that is sufficient to satisfy the conditions that establish the proposal, as a condition of effectiveness that guarantees the cryptographic environment. This effectiveness implies that the detection order finalizes the endpoints, the communication, which is cryptographic and must be modified in order to have

66Council of the European Union, Opinion of the Legal Service, op. cit., parr. 44-48.

the objective of providing, investigating and analyzing the content in transit of communications via the servers[67].

Personal data takes into account the abandonment of end-to-end encryption and/or, which introduces a back-door that accesses the cryptographic content. The use of client-side scanning is invasive[68] and transforms the transmission to surveillance of mass (Abelson and others, 2021)[69].

The risk of exploitation of encryption by others includes intelligence agencies and criminal organizations (Abelson and others, 2015). As security measures, the substance of the right to protection of personal data is guaranteed according to Art. 8 CFREU (Peers and others, 2021). Some technical solutions guarantee and protect the confidentiality of electronic communications, which include encryption measures that are essential to guarantee the enjoyment of fundamental rights[70].

The communication of personal data to a third party as well as the public authority, is part of an interference with the fundamental rights of Articles 7 and 8 CFREU (Peers and

67Opinion of the Legal Service, Proposal for a Regulation laying down rules to prevent and combat child sexual abuse-detection orders in interpersonal communications. Articles 7 and 8 of the Charter of Fundamental Rights-Right to privacy and protection of personal data-proportionality, op. cit., par. 17.

68Business Social Responsibility (BSR), Human Rights Impact Assessment, Meta's Expansion of End-to-End Encryption, 4 April 2022.

69Signal Foundation, Meredith Whittaker: EDRi, President of Signal Foundation Meredith Whittaker's speech for EDRi's 20th anniversary, 13 April 2023.

70Human Rights Council, Resolution 47/16 on the Promotion, Protection and Enjoyment of Human Rights on the Internet, UN Doc. A/HRC/RES/47/16, 26 July 2021, p. 2.

others, 2021),which goes beyond the use of the communicated information and this also applies to the storage of personal data as well as to their use by public authorities[71]. Information that has to do with private life is sensitive information that concerns possible inconveniences[72].

A regulation allows public authorities to have access in a generalized manner to the content of electronic communications that could jeopardize the essential content of the rights considered[73]. The need to make changes to the generalized access of the content of communications it was envisaged by the CSAM proposal, especially in consideration of the possible compromise of the essence of the right to respect private life as well as the right to protect personal data.

The technology which the provider may use must not be able to extract different information from the relevant communications, i.e. from those strictly necessary to detect CSAM. It must be compliant with the state of the article in the sector and to be as least intrusive as possible in terms of impact on users' rights to privacy and family life, as well as data protection. This does not in itself exclude the risk that the automated analysis involves all

71CJEU, joined cases C-362/14 and C-362/14, Maximilian Schrems v. Data Protection Commissioner-Digital Rights Ireland Ltd of 6 October 2015, op. cit., parr. 33-35 and 87.

72CJEU, C-817/19, Ligue des droits humains ASBL v. Conseil des ministres of 21 June 2022, op. cit., par. 96.

73CJEU, joined cases C-362/14 and C-362/14, Maximilian Schrems v. Data Protection Commissioner-Digital Rights Ireland Ltd of 6 October 2015, op. cit., par. 94.

the communication data of each user of the service to whom the order is addressed, without even a direct or indirect connection with crimes of sexual abuse of minors[74].

The risk of interference according to Articles 7 and 8 CFREU (Peers and others, 2021) establishes a surveillance system of a general nature, which systematically indiscriminates the automatic evaluation of personal data, where users use interpersonal communication services[75].

Objectives pursued and proportionality of the CSAM proposal

Some limits are foreseen in terms of proportionality to the rights that the CFREU establishes (Peers and others, 2021) which exceed the limits that are suitable for achieving the legitimate and pursued objectives, available to appropriate measures that restrict disproportions compared to their chosen objectives from the same proposal[76].

In this respect, the methodology develops and is based on the jurisprudence of the CJEU to evaluate the interferences that proportionally affect fundamental rights in data observations and access to metadata.

74Art. 10, par. 3, lett. b), c) and d) of the proposal of Regulation.

75CJEU, C-817/19, Ligue des droits humains ASBL v. Conseil des ministres of 21 June 2022, op. cit., parr. 92 to 111.

76CJEU, C-336/19, Centraal Israëlitisch Consistorie van België and others of 17 December 2020, ECLI:EU:C:2020:1031, not yet published, par. 64.

In particular, the CJEU stated that:

"(...) in Articles 7, 8, 11 and 52, par. 1 of the Charter do not preclude legislative measures which, for the purposes of fighting serious crime and preventing serious threats to public security, provide for targeted retention of traffic data and location data which is delimited, on the basis of objective and non-discriminatory elements, based on the categories of people interested or through a geographical criterion, for a period limited to what is strictly necessary"[77].

The positive obligations that may derive from Articles 3, 4 and 7 of the Charter concern the establishment of rules, which allow an effective fight against crimes that cannot have the effect of justifying an interference entailed in legislation and providing for the retention of the relevant data traffic and the location data of the fundamental rights enshrined in Articles 7 and 8 of the Charter, without the data of the interested parties being capable of revealing a connection, at least indirect, with the objective pursued[78].

EU law does not preclude, for the purposes of fighting crime in general, the generalized retention of data relating to personal identity and IP addresses[79]. The conservation of the IP addresses of all natural persons, who own equipment that allows access to the Internet could be the only means of investigating crimes committed online, even in cases of particularly serious child

77CJEU, joined cases C-793/19 and C-794/19, Bundesrepublik Deutschland v. SpaceNet AG and Telekom Deutschland GmbH of 20 September 2022, ECLI:EU:C:2022:702, not yet published, par. 75.

78CJEU, joined cases: C-511/18, C-512/18 and C-520/20, La Quadrature du Net and others v. Premier ministre and others of 6 October 2020, op. cit., par. 145.

79CJEU, joined cases C-793/19 and C-794/19, Bundesrepublik Deutschland v. SpaceNet AG and Telekom Deutschland GmbH of 20 September 2022, op. cit., par. 99.

pornography crimes, such as the acquisition, dissemination, transmission or making available online of child pornography material, pursuant to Art. 2, letter. c), of Directive 2011/93/EU.

The personal identity of users, in addition to contact data, such as their addresses, does not provide any information on the communications sent and, consequently, on the privacy of users. The interference resulting from the conservation of such data cannot, in principle, be considered serious.

IP addresses, although part of traffic data, do not reveal, as such, any information relating to third parties subjects, who have been in contact with the person, who made the communication. This category of data is therefore less sensitive than other data relating to traffic[80]. The serious interference determined by the generalized automated analysis of data relating to traffic and location can satisfy the proportionality requirement only in situations where there is a serious threat to national security, which is demonstrated to be real and present or foreseeable, and providing that the duration of such retention is limited to what is strictly necessary.

In similar circumstances a general and indiscriminate evaluation of data suitable for revealing the nature of the information consulted online and which is applied independently of a connection, even indirect or remote, with illicit activities, can be

80CJEU, joined cases: C-511/18, C-512/18 and C-520/20, La Quadrature du Net and others v. Premier ministre and others of 6 October 2020, op. cit., parr. 152-158.

justified in light of the requirements deriving from Articles 7, 8 and 11 and by art. 52, par. 1, of the Charter[81].

The criteria just mentioned do not appear to be conclusive within the proposed CSAM regulation. The detection orders indicate that communications are examined for the presence of child pornography and the solicitation of minors.

Within this context, the CJEU, through the Commissioner of An Garda Síochána, affirmed that:

"(...) a conservation measure can be considered justified only if "targeted", i.e. only if it is based on objective and non-discriminatory criteria and addresses those subjects whose data are suitable to reveal a connection, at least indirect, with acts of serious crime and, in particular, those previously identified as a threat to public safety or national security" (paragraphs 76, 77 and 78)[82].

It does not provide for a detailed indication of the recipients whose communications should be monitored. The measure does not constitute a form of "targeted" surveillance, therefore being disproportionate to the aim pursued. A disproportion further aggravated by the duration of the survey, given that, pursuant to Art. 7, par. 9 of the CSAM proposal, the period of application of the order for the detection of child pornography and cases of solicitation can last, respectively, 12 and 24 months given the

81CJEU, joined cases: C-511/18, C-512/18 and C-520/20, La Quadrature du Net and others v. Premier ministre and others of 6 October 2020, op. cit., parr. 172-178.

82CJEU, C-140/20, G.D. v. The Commissioner of An Garda Síochána and others of 5 April 2022, ECLI:EU:C:2022:258. joined cases: C-511/18, C-512/18 and C-520/20, La Quadrature du Net and others v. Premier ministre and others of 6 October 2020, op. cit., par. 148-149. C-203/15 and C-698/15, Tele2 Sverige AB v. Post-och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and others of 21 December 2016, op. cit., parr. 110-111.

considerable duration of the monitoring period.

A reevaluation is not envisaged of the necessity of the provision nor a limit on its possible renewal; a circumstance which opens up the risk of giving rise to surveillance which, in addition to being generalized and indiscriminate, could also take on a permanent nature[83].

As regards the issue of proportionality, it is worrying and considers the level of sensitivity of data and interpersonal communications that derive information that is related to the personality of the person concerned as well as social relationships and daily activities. It is not easy to understand the rich jurisprudence just cited justifying the provision which aims to combat the related crimes, that are indisputable and not linked to threats and national security.

In this regard, the CJEU states that:

"(...) the objective of preserving national security corresponds to the primary interest of protecting the essential functions of the state and the fundamental interests of society through the prevention and repression of activities that may destabilize the fundamental constitutional, political, economic or social structures of a country, and in particular to threaten society, the population or the state as such, such as in particular terrorist activities"[84].

Unlike crime, even particularly serious, a threat to national

83European Parliamentary Research Service, Proposal for a Regulation Laying Down the Rules to Prevent and combat Child Sexual Abuse. Complementary Impact Assessment, April 2023, reperibile online: https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2023)740248 p. 59-61.

84CJEU, joined cases: C-511/18, C-512/18 and C-520/20, La Quadrature du Net and others v. Premier ministre and others of 6 October 2020, op. cit., par. 135. C-140/20, Commissioner of An Garda Síochána of 5 April 2022, ECLI:EU:C:2022:258, not yet published, par. 61.

security must be real and current or, at least, foreseeable, a circumstance which presupposes the occurrence of sufficiently concrete circumstances to be able to justify a measure of generalized and undifferentiated conservation of traffic data and location data, for a limited period. The distinction between a similar threat, characterized by a particular nature, gravity and specificity, by the risk of tensions or disturbances, even serious, of public security or by the risk of serious crimes, including abuse sexual acts on minors[85].

It is understood that the conservation of metadata, according to the cited jurisprudence, is part of a proportionate justice, where the purposes of safeguarding national security does not appear as screening of a content of interpersonal communications through online sexual abuse of minors and which prefigure the CSAM proposal as well as the importance of the objectives it sets, without proportioning data of a different nature to a crime, that respects the threats posed to national security, revealing it as likely to undermine the essence of the relevant rights of reference.

Concluding remarks

When we talk about minors and sexual abuse on the Internet we

85CJEU, joined cases: C-511/18, C-512/18 and C-520/20, La Quadrature du Net and others v. Premier ministre and others of 6 October 2020, op. cit., parr. 136-137. C-140/20, Commissioner of An Garda Síochána of 5 April 2022, op. cit., par. 62.

mean of vulnerable people who are exposed to risks of various kinds. For this reason, is necessary to provide actions that guarantees protection on the Internet through essential measures. As we understood from the investigation above, the EU has adopted soft law acts and has also developed various measures in time of a binding nature in order to create a digital environment starting from Directive 2011/93/EC, ensuring the protection of minors and all forms of violence, which has favored contrasting rules of sexual abuse by fueling the evolution of rules that are in conflict with the access and diffusion of child pornography material.

Cyberspace has been addressed by the European Commission through the adoption of legislation that digitally determines the protection of minors' rights by establishing greater responsibility for providers of communication services and hosting services. The current system is based on a voluntary basis in cases of online sexual abuse by companies that reveal that the adequate protection of children is insufficient, of the communication service providers that fall within the application of the ePrivacy Directive and of the legal basis, that is necessary by continuing to implement voluntary activities, within the expiry of EU Regulation 2021/1232, which is scheduled for 3 August 2024.

The proposed CSAM Regulation aims first of all to remove the temporary nature of the system in force up to now by trying to

harmonize and combat sexual abuse against minors and the improper use of ICT services by imposing evaluation services and obligations on providers and risk mitigation to similar use of detection, blocking and removal in cases of child pornography and grooming.

ICT service providers fall within the scope of application of the legislation certainly through various doubts related to the scope of application of the legislation as well as doubts concerning the obligation of detection, which constitutes measures of last resort, i.e. preventive measures of mitigation, that are demonstrated as ineffective.

We believe that the doubts comply with the order of detection, with Art. 7 of the CSAM proposal and with Articles 7, 8 and 11 CFREU (Peers and others, 2021) for the protection of privacy, the protection of personal data and freedom of expression. The prevention and fight against sexual abuse of minors constitutes an objective of general interest. Also, the formulation of a regulation introduces limits to the rights that are indicated to satisfy the requirements of Art. 52, par. 1 CFREU (Peers and others, 2021).

The proposed regulation aims to establish a harmonized legal framework for the online child sexual abuse, which certainly guarantees service providers by establishing a fair balance between protection measures for minors and their own rights

and the fundamental rights of other users and of providers by observing a current formulation of the legislation, which has and presents multiple elements, that prevent the preparation of an adequate budget, which is always under continuous investigation.

The same measures contribute to and reduce the possibilities for children, who are victims of online sexual abuse to present a risk for the protection of their privacy rights and their freedom of expression.

The fear of the authorities on the control of data protection and legal services, which involve all the European institutions in the process of adopting the act that respects the risk with adequate guarantees of protection of privacy and personal data, opens the door to mass surveillance, which shares the same subjects according to the legislation to protect. Monitoring this age is not very easy and perhaps compromises one's freedom of expression and the possibility of exploring one's sexuality (Beyer, 2012).

The proposed CSAM Regulation[86] is part of the positions of the European Commission and in accordance with the legitimacy and proportionality of the detection orders in the CSAM, which are based on the rights at stake and the absolute rights that are

86EDRi. (2023, July, 4). Despite warning from lawyers, EU Governments Push for Mass Surveillance of our Digital Private Lives: https://edri.org/our-work/despite-warning-from-lawyers-eu-governments-push-for-mass-surveillance-of-our-digital-private-lives/

considered in their social function[87]. This is a circumstance that justifies the structure of the legislation under consideration. Some of the Member States, even a few, continue to see the need for a substantial modification of the legislation in question, towards a greater level of protection of minors in cyberspace, which corresponds to the guarantee of adequate protection of further fundamental rights and freedoms, that are involved in this particular topic[88].

87Commission Services, Proposal for a Regulation of the European Parliament and of the Council Laying Down Rules to Prevent and Combat Child Sexual Abuse-Balancing the Rights of Children with Users' Rights, 2022/0155(COD), Bruxelles, 16 May 2023, p. 3-4.

88See the resolution of the French Senate of 20 March 2023, Résolution européenne sur la proposition de règlament du Parlament européen et du Conseil établissant des règles en vue de prévenir et de combattre lesa bus sexuals sur enfents-COM(2022)209 final, No. 77. The resolution of the Austrian Parliament of 3 November 2022, Binding Resolution of the Austrian Parliament against the Child Sexual Abuse Regulation. The communication of the German Bundestag of 1 March 2023, Sachverständige üben breite Kritik an Plänen zur Chatkontrolle. The letter from the Irish Houses of the Oireachtas of March 2023, Political Contribution on Proposal for a Regulation of the European Parliament and of the Council Laying Down Rules to Prevent and Combat Child Sexual Abuse.

References

Abelson H. and others. (2015, July, 15). Keys under doormats: Mandating insecurity by requiring government access to all data and communications. *Journal of Cybersecurity, 1 (1).*72ss.

Abelson, H. and others. (2021, October, 14). Bugs in our pockets: The risks of client-side scanning. *ArXiv*: https://arxiv.org/abs/2110.07450

Ali, S., Abou Hayykal H., Youssef, E. (2021). Child sexual abuse and the internet. A systematic review. *Human Arenas, 4 (1),* 405ss.

Bellanova, R., De Goede, M. (2022). Co-producing security: Platform content moderation and European security integration. *Journal of Common Market Studies, 60 (5),* 1319ss.

Beyer, P. (2012, March, 7) #ChatControl survey: Children don't want to be "protected" by scanning or age-restricting messenger and chat apps: https://www.patrick-breyer.de/en/chatcontrol-survey-children-dont-want-to-be-protected-by-scanning-or-age-restricting-messenger-and-chat-apps

Bignami, F. (2006). Protecting privacy against the police in the European Union: The Data Retention Directive. In Y. Bot, *Melanges en l'honneur de Philippe Léger.* ed. Pedone, Paris, 111ss.

Blanke, H.J., Mangiamelli, S. (2021). *Treaty on the Functioning of the European Union. A commentary,* ed. Springer, Berlin.

Brkan, M. (2018). The concept of fundamental rights in the EU legal order: Peeling the onion to its core. *European Constitutional Law Review, 14 (2),* 333ss.

Cameron, I. (2021). Metadata retention and national security: Privacy international and La Quadrature du Net. *Common Market Law Review, 58 (5),* 1434ss.

Chander, A. (2020). Is data localization a solution for Schrems II?. *Journal of International Economic Law, 23,* 772ss.

Christakis, T. (2020, July, 21). After Schrems II: Uncertainties on the legal basis for data transfers and constitutional implications for Europe. *Europeanlawblog.eu*: https://europeanlawblog.eu/2020/07/21/after-schrems-ii-uncertainties-on-the-legal-basis-for-data-transfers-and-constitutional-implications-for-europe/

Davis, M. (2023). Internet cookies in European Union (EU) law. *Juris Gradibus, 2(1),* 38-64.

De Sstreel, A. (2020, June). Online platforms' moderation of illegal content online. Law, practice and options for reform: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/652718/IPOL_STU(2020)652718_EN.pdf;

Dhont, J.H. (2019). Schrems II. The EU adequacy regime in existential crisis?. *Maastricht Journal of European and Comparative Law, 5,* 598ss.

Dorotic, M., Johnsen, W. (2023). Child sexual abuse on the

internet report on the analysis of technological factors that affect the creation and sharing of child sexual abuse material on the internet. *Norwegian Business School, research series, n. 1:* https://biopen.bi.no/bi-xmlui/bitstream/handle/11250/3055430/SOBIrapport_finalversion_BIOpen.pdf?sequence=1

Dunn, P., De Gregorio, G. (2023, April 23). A new tile for the EU content moderation governance mosaic? The proposal for a child sexual abuse material regulation. *MediaLaws*: https://www.medialaws.eu/a-new-tile-for-the-eu-content-moderation-governance-mosaic-the-proposal-for-a-child-sexual-abuse-material-regulation/

Feiler, L. (2010). The legality of the Data Retention Directive in light of the fundamental rights to privacy and data protection. *European Journal of Law and Technology, 1 (3),* 4ss.

Flett, E., Wilson, J., Clover, J. (2020). Schrems strikes again: EU-US privacy Shield suffers same fate as its predecessor. *Computer and Telecommunication Law Review, 6,* 162ss.

Garde, A. (2014). Children and the European Union. Rights, welfare and accountability. *Children and Society, 28 (6)*, 9ss.

Gonzàlez Fuster, L. (2014). *The emergence of personal data protection as a fundamental right of the EU.* ed. Springer, Cham

Granger, M., Irion, K. (2014). The Court of Justice and the

Data Retention Directive in digital rights Ireland: Telling off the EU legislator and teaching a lesson in privacy and Data Protection. *European Law Review, 6,* 850ss.

Guild, E., Carrera, S. (2014). The political and judicial life of metadata: Digital rights Ireland and the trial of the Data Retention Directive. *CEPS Paper in Liberty and Security in Europe*, 8ss.

Jones, C., Hayes, B. (2013). The EU Data Retention Directive: A case study in the legitimacy and effectiveness of EU counterterrorism policy. In Securing Europe through counter-terrorism-impact, legitimacy and effectiveness: https://www.europarl.europa.eu/RegData/etudes/STUD/2022/730581/IPOL_STU(2022)730581(SUM01)_EN.pdf

Kilkelly, U., Liefaard, T. (2020). *International human rights of children.* ed. Springer, Berlin.

Kisunaite, A., Delicati, S. (2021). The European Union and the United Nations Convention on the Rights of the Child. Towards a fully-fledged European Union child rights strategy. In E. Marrus, P. Laufer-Ukeles (eds). *Global reflections on children's rights and the law. 30 years after the Convention on the Rights of the Child.* ed. Routledge, New York, 48ss.

Koenig, C., Bartosch, A., Braun, J.D., Romes, M. (2009). *EC competition and telecommunications law.* Kluwer Law International, Alphen aan den Rijn.

Kornelius, W. (2023). Prior filtering obligations after Case C-401/19: balancing the content moderation triangle A comparative analysis of the legal implications of Case C-401/19 for filtering obligations ex ante and the freedom of expression in Europe. *JIPITEC-Journal of Intellectual Property, Information Technology and E-Commerce Law, 14,* 123ss.

Lenaerts, K (2019). Limits on limitations: The essence of fundamental rights in the EU. *German Law Journal, 20,* 773ss.

Liakopoulos, D. (2019). Regulation (EU) 2016/679 on the protection of personal data in light of the "Cambridge Analytica" affair. *E-Journal of Law. An independent law Journal, 5 (1).*

Lind-Haldorsson, A., O'Donnell, A. (2015). The EU and Child protection systems: The role and the impact of the EU in advancing children's protection rights. In I. Iusmen, H. Stalford (eds). *The EU as a children's rights actor. Law, policy and structural dimension.* Verlag Barbara Burdich, Lancaster, 102ss.

Liss, J., Peloquin, D., Barnes, M., Bierer B.E. (2021). Demystifying Schrems II for the cross-border transfer of clinical research data. *Journal of Law and the Biosciences*, 8, (2).

Lutkevich, B., Bacon, M. (2021, June). End-to-end encryption (E2EE). *Techtarget*: https://www.techtarget.com/searchsecurity/definition/end-to-end-encryption-E2EE.

Martellozzo, E. (2012). *Grooming, policing and child protection in a multi-media world.* ed. Routledge. New York.

Menn, J. (2012, July, 12). Social networks scan for sexual predators, with uneven results. *Reuters:* https://www.reuters.com/article/oukin-uk-usa-internet-predators-idUKBRE86B05M20120712

Nunziato, D.C. (2023). The digital services act and the Brussels effect on platform content moderation. GWU Legal Studies Research Paper No. 2023-28. *GWU Law School Public Law Research Paper No. 2023-28.*

Peers, S. and others (eds.). (2021). *The EU Charter of Fundamental Rights. A commentary*. Hart Publishing, Nomos, C.H. Beck, Oxford & Oregon, Portland.

Ramiro, L.S. and others. (2019). Online child sexual exploitation and abuse. A community diagnosis using the social norms theory. *Chils Abuse & Neglect, 96.*

Royer, S., Careel, S. (2021, March, 23). Access denied. CJEU reaffirms La Quadrature du Net and clarify requirements for access to retained data, *CITIP:* https://www.law.kuleuven.be/citip/blog/access-denied-cjeu-reaffirms-la-quadrature-du-net-and-clarifies-requirements-for-access-to-retained-data/

Sajfert, J. (2020, October, 26). Bulk data interception/retention judgments of the CJEU. A victory and a defeat for privacy.

European Law Blog: https://europeanlawblog.eu/2020/10/26/bulk-data-interception-retention-judgments-of-the-cjeu-a-victory-and-a-defeat-for-privacy/

Sartor, G., Loreggia, A. (2022). *The impact of pegasus on fundamental rights and democratic processes. Study requested by the European Parliament's PEGA Committee:* https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2022)740514

Shuterland, E.E. (2016). *Implementing article 3 of the United Nations Convention on the Rights of the Child. Best interest, welfare and wellbeing.* Cambridge University Press, Cambridge.

Simon, D. (2020). Coup de tonnerre dans le monde du numérique. *Europe, 8-9,* pp. 7ss.

Svantesson, D. (2016). The CJEU's Weltimmo data privacy ruling: Lost in the data privacy turmoil, yet so very important case C-230/14, Weltimmo, EU:C:2015:639. *Maastricht Journal of European and Comparative Law, 2,* 334ss.

Taddeo, M., Floridi, L., (2017). *The responsibilities of online service providers*. ed. Springer, Berlin.

Taylor, M. (2006). The EU Data Retention Directive. *Computer Law and Security Report, 22 (4),* 312ss.

Tracol, X. (2020). "Schrems II": The return of the privacy shield. *Computer Law & Security Review, 39,* pp. 4ss.

Tracol, X. (2021, July). The two judgments of the European Court of Justice in the four cases of privacy international, La Quadrature du Net and others, French Data Network and others and Ordre des Barreaux francophones et germanophone and others: The Grand Chamber is trying to hard to square the circle of data retention. *Computer Law and Security Review, 6 (1)*, 1-13.

Van Daalen, O. (2022, June, 7). Does monitoring your phone affect the essence of privacy?. *European Law Blog:* https://europeanlawblog.eu/2022/06/07/does-monitoring-your-phone-affect-the-essence-of-privacy/

Vandenhole, W., Türkelli, E.L., Lelmbrechts, S. (2019). *Children's rights. A commentary on the Convention on the Rights of the Child and its Protocols.* Edward Elgar Publishers, Cheltenham.

Voigt, P., Von Dem Bussche, A. (2017). *The European Union General Data Protection Regulation (GDPR): A practical guide.* ed. Springer, Berlin, 23ss.

Voss, W.G. (2020). Cross-border data flows, the GDPR, and data governance. *Washington International Law Journal, 30 (3),* 485ss.

Wakefield, J. (2021, September, 3). Apple delays plan to scan iPhones for child abuse. *CNBC:* https://www.cnbc.com/2021/09/03/apple-delays-controversial-

plan-to-scan-iphones-for-child-exploitation-images.html

Wilman, F. (2020). *The responsibility of online intermediaries for illegal user content in the EU and in the US.* Edward Elgar Publishers, Cheltenham.

Woods, L. (2020, December, 16). Overview of digital service act. *EU Law Analysis:* https://eulawanalysis.blogspot.com/2020/12/overview-of-digital-services-act.html

Zech, H. (2021, September, 2). General and specific monitoring obligations in the digital services act. *Verfassungsblog:* https://verfassungsblog.de/power-dsa-dma-07/